

REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

With respect to consideration of the references cited in the International Search Report (ISR), it is noted that the acceptance letter from the U.S. Patent and Trademark Office mailed 04/19/2002 acknowledges receipt of the ISR and of a copy of each reference therein cited. Although it is understood that the listing in the ISR is not the preferred format for such listing, given the Examiner's examination duties, at least consideration of the documents already present in the file was expected (even if the printing of such references on the face of the patent might not be expected unless a suitable convenient format for the listing of these references was timely provided by the applicant or the listing was made by the Examiner on the Form PTO-892).

In any event, for the Examiner's convenience, a suitable Form PTO-1449 is now attached to provide the requisite format for the listing of these references now long present in the U.S. Patent and Trademark Office file wrapper for this case. Since consideration of these references should already have been made, it is respectfully submitted that no further IDS fee should be required for completing the record in the case to cause the printing of these references on the face of any issued patent. However, if such additional IDS fee is, upon reconsideration, deemed necessary, then authority is hereby given to charge such fee to our Account No. 14-1140.

Return of a fully initialed copy of the Form PTO-1449 is respectfully requested.

In response to the formality-based objections, the entire application has been reviewed and revised above so as to obviate all such objections and place this application in more traditional US format.

The rejection of claims 1-11 under 35 U.S.C. §102 as allegedly anticipated by Perlman '865 is respectfully traversed.

The term "distinct data elements" in claim 1, step (i) has been replaced with the term "unique random numbers". Support for this amendment can be found in steps 105-115 of the Figure 1a in the corresponding text on page 8, lines 5-19. Furthermore, in claim 1, step (iii), the "unused data elements" that was selected has been replaced with "a random number" that is selected, wherein said "selected random number" is further defined as having "not previously been selected and not previously been included in a data packet to be sent". This amendment merely clarifies the fact that a random number is selected from the earlier stored and sent list, where the random number has not previously been selected for use. Support for this amendment can be found in steps 205 and 210 of Figure 2, and in the corresponding text on page 9, lines 4-12.

Claim 2 has also been amended to more clearly define the feature in step 6, so that it better corresponds with the feature of step 225 in Figure 2a and as described on page 10, lines 17-20.

The other corresponding independent claims directed towards the authorized recipient server (claim 4), the apparatus of the first server and (claim 6) and the apparatus of the second server (claim 10) have also been amended in line with claim 1.

The present invention relates to a method for transmitting data packets between a first server to an authorized recipient server in a manner that enables the authorized recipient server to check that the data packet has indeed originated from the first server. The method advantageously does not have the processing overheads associated with digital signature techniques and other previously recognized techniques. Exemplary embodiments use a list of random numbers generated by the first server, which are shared between the two servers (see steps (i) and (ii) of claim 1) by sending the list from the first server to the recipient server. A random number is then selected from the list by the first server for including in a data packet to be sent from the first server to the authorized recipient server, wherein the random number selected is not one that has been previously selected and subsequently included in a previously sent data packet (see step (iii) of claim 1).

By adopting the steps (i) to (iv) of claim 1, the recipient server can determine if the data packets were received from the first server. This is because the list of unique random numbers is securely shared between the first server and the authorized recipient server, and thus, a third party attempting to send false data packets to the authorized recipient server would need to guess exactly what random numbers are in the list to use for transmission in a data packet, and he would not be able to use previously used ones.

Such exemplary embodiments are particularly advantageous over known authentication techniques where individual data packets are encrypted and decrypted, because each data packet can be sent unencrypted. The verification performed by the authorized recipient server in the invention is merely checking that the random number used in the data packet is one that is in the

list of unique random numbers that were sent by the first server to the authorized recipient server over secure communication means, and that the random number has not previously been used. As such, the more significant processing overhead of receiving the list of unique random numbers over a secure communication means need only be performed once until the list of random numbers is exhausted.

It should be clear from the general description that such a method is relatively secure, especially if the random numbers are large and a relatively small list is generated. For example, on page 8, lines 5 to 14, 24-bits of random numbers are proposed to give more than 16.7 million different random numbers and where only perhaps 1000 of those possible 16.7 million numbers are actually used in a particular list. A third party attacker would therefore struggle to predict which 1000 of those 16.7 million have been generated by the first server and communicated, by secure means, to the authorized recipient server for use in transmitting data packets between the two parties.

Perlman describes a method and system for transmitting data packets between interconnected nodes using public/private key encryption. The methods in Perlman are significantly more complex from a computational perspective than that of the present invention. As already mentioned, the way in which data packets are transmitted between nodes in Perlman is based on the well-known public/private key system. However, before such a system can be utilized, the node ID and associated public key for each node in the network must be transmitted to every other node, so that when one of the nodes wishes to transmit data to another node, it encrypts the data using the public key associated with the destination node. The destination node

can then decrypt the data using its private key. Therefore, Perlman describes a procedure for propagating the node ID and associated public key in a public key list (PKL) for use in subsequent data transmissions. This set-up procedure is also used to explore the network topology. The text identified by the Examiner in relation to claim 1 from Perlman relates to the distribution of the PKL between the nodes so that each node has the public key associated with every other node in the network and can also determine the topology of the network so that route selection for data transmission can be optimized.

Now that claim 1 has been amended to require that random numbers be generated by the first server and sent to a recipient server in a list, and then that these random numbers are used only once in the sending of subsequent data packets from the first server to the recipient server, it should be clear that Perlman is no longer particularly relevant.

Specifically, the only reference in Perlman of generating any numbers for use in transmission in data packets is the sequence number 74, which is used to determine if a packet is outdated or not (see column 6, lines 17 to 22). Therefore, if the PKL at a particular node is unchanged, then it will send the LSP packet with the same sequence number as one used previously. This differs significantly from the use of random numbers in claim 1 of the present invention, wherein a series of random numbers are stored as a list at the first server and sent to the recipient server, and then subsequently used only once in transmitting a data packet. The sequence number in Perlman is neither a random number nor does it need to be as it is not used in the same manner as in the present invention for identifying the source of the data packet

transmitted. Furthermore, the sequence number is not transmitted in any list prior to its use in the transmission of a data packet as defined in claim 1 of the present invention.

One significant advantage of the present invention is that processing overheads are significantly reduced as authentication of the source (first server) in the present invention is based on cross checking of the received random number in the received data packets against the previously received list of random numbers. In contrast, authentication of data packets in Perlman relies on the use of digital signature and/or public/private key encryption. This is because the operation of the present invention differs significantly from the approach taken in Perlman. As such, there is no motivation to modify the teachings of Perlman to arrive at the teachings of the present invention.

In the Examiner's specific objections to claim 1, the list of random numbers that is sent to the recipient server from the first server is by secure communication means. The Examiner has cited in Perlman to the use of private and public keys in column 5, as anticipating this feature. Firstly, the list that is sent merely includes the node IDs and associated keys for each node and not a list of "unique random numbers" as defined in claim 1. Secondly, the public key list is not sent to neighboring nodes over secure communications means as alleged by the Examiner. The PKL comprises public keys, which are designed to be snared and available to everyone without the need to further encrypt them or the list they reside in. This is a well known feature of public/private key authentication.

In summary, Perlman fails to specifically disclose the two-step approach of sending a random number list between two servers and then using random numbers from that list in subsequently transmitted data packets to ensure the integrity of the sender.

Therefore, claim 1 as amended is both novel and non-obvious over Perlman.

With reference to claim 2, the text cited by the Examiner from column 9 of Perlman relates to a different embodiment of Perlman to the text cited against claim 1, and therefore cannot be combined with the earlier references in relation to claim 1 unless the Examiner can specify some specific motivation to do so (see column 9, lines 33-36, which highlights the fact that this refers to an alternative method). In any case, even if the Examiner were to combine the different embodiments of Perlman, the text cited by the Examiner still fails to disclose all the additional features of claim 2 and specifically step (vi) of claim 2. Step (vi) of claim 2 identifies the position of the random number selected in step (iii) (used in a received data packet), and then compares this position with the sequence number (i.e., position) receives from step (v), to check that the authorized recipient server is indeed authorized and not an unauthorized third party server. This is possible because only authorized recipient servers will possess the correct random number list and therefore only authorized recipient servers can correctly determine the position of a random number in that list that was used in a received data packet (see page 10, lines 17-27). This is entirely different to the text cited by the Examiner which relates to retransmission of data packets to avoid failed nodes or routes. The list highlighted by the Examiner in this text corresponds to a list of ID numbers, and alleges that the position of these ID numbers can inherently be determined, are firstly not equivalent to the random numbers of

EVANS et al
Appl. No. 10/049,844
October 26, 2005

claim 1, and secondly the positions of these ID numbers are certainly not cross-referenced with the positions in the original PKL list in order to determine whether a data packet should be resent as defined in step (viii).

Therefore, claim 2 is also novel and non-obvious over Perlman.

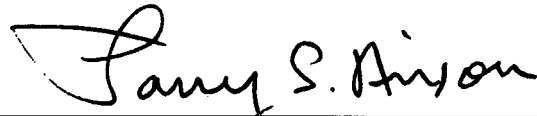
As corresponding claims 4, 6 and 10 define some similar features as claim 1, these are also novel and non-obvious for reasons similar to those already stated.

Accordingly, this entire application is now believed to be in allowable form and a formal Notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By:



Larry S. Nixon
Reg. No. 25,640

LSN:vc
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100